UNITED STATES PATENT AND TRADEMARK OFFICE

MN

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,415	02/01/2002	Ahmet Mursit Eskicioglu	RCA 89462	3679

7590	03/16/2007

Joseph S Tripoli
Thomson Multimedia Licensing Inc
PO Box 5312
Princeton, NJ 08543-5312

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	09/936,415	ESKICIOGLU ET AL.
	Examiner	Art Unit
	Longbit Chai	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _07 February 2005_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-8,10,14 and 17-24_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-8,10,14 and 17-24_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _01 February 2002_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Original application contained claims 1 – 20. Claims 9, 11 – 13 and 15 – 16 are

cancelled and new claims 21 – 24 are added in the amendment filed on 2/7/2007.

Presently, pending claims are 1 – 8, 10, 14 and 17 – 24.

Response to Arguments

2.   As per claim 1, 10 and 17, Applicant asserts that (a) a combination of Tsuria in

view of En-Seung fails to teach or suggest "a rebundled descrambling key that is

rebundled using a key associated with a first device, or access device, as recited in

independent claims 1, 10 and 17 (Remarks; Page 9 / 3rd Para)" and (b) En-Seung

teaches "the use of user keys associated with specific users to encrypt the temporary

validation key, while Tsuria discloses generating TECM based on the access device

(Remarks; Page 11 / 1st Para Line 1 – 4)". Examiner respectfully disagrees with the

following reasons:

- Regarding the argument, a rebundled descrambling key which is rebundled

    using a key associated with the terminal unit (i.e. the 2nd device), Examiner notes

    in the encryption / decryption mechanism, the 1st device and the 2nd device are

    functionally bundled together in order to encrypt / decrypt the digital content – i.e.

    both of then can not be separated and functioned independently. Besides, the

    user is the customer for both of the 1st device (e.g., IRD or Setup Box) as well as

    the 2nd device (e.g., presentation device) and therefore the user (customer)

information or the user (customer) key is indeed associated with both of the 1st

device and the 2nd device in view of the TECM key (i.e. transformed ECM key or

rebundled descrambling key). Besides, En-Seung teaches the first device (i.e.

the server or the access device) can also generate the key information related to

the users in the decryption process as well as in the encryption process (En-

Seung: Column 4 Line 58 – 63) in correspondence with the user's (i.e.

customer's) identity characters for the terminal unit (i.e. the 2nd device or the

presentation device) and Tsuria teaches TECM key may be associated with a

combination of the IRD (i.e. the 1st device) as well as a smart card and the TECM

key may be personal to a particular user (customer) of the apparatus (i.e. the 1st

device (or access device) and the 2nd device (i.e. the presentation device)

(Tsuria: Column 8 Line 53 – 62) and as such Tsuria in view of En-Seung does

teach "a rebundled descrambling key that is rebundled using a key associated

with a first device, or access device".

• Besides, Tsuria teaches a public / private key-pair can be used in the

conditional access system for providing proof of authenticity to the receiving

decoder (i.e. the 2nd device) and therefore the unique key associated with the first

device can be obviously used as a public / private key located in the first device

and a corresponding private / public key (as a counter-part) being obviously

located in the second device (Tsuria: Column 3 Line 1 – 8, Column 8 Line 53 –

55 and Column 7 Line 5: See commonly assigned <both are from the same assignee

NDS Ltd. Inc.> and fully incorporated into Tsuria by reference the U.S. Patent

5,481,609, to Cohen et al., Column 1 Line 62 – 67).

• Therefore, Tsuria in view of En-Seung teaches the TECM key (i.e. a

rebundled descrambling key) is not only associated with the 1st device but also

associated with the 2nd device as a whole to enable the encryption / decryption

functions work seamlessly.

• Furthermore, Examiner notes, according to MPEP § 2145, one cannot show

nonobviousness by attacking references individually where the rejections are

based on combinations of references. In re Keller, 642 F.2d 413, 208 USPQ 871

(CCPA 1981); In re Merck & Co., Inc., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

1986). Tsuria reference is relied upon providing rebundling, in said first device,

said descrambling key using a unique key associated with said first device

(Tsuria: Column 3 Line 1 – 8 and Column 8 Line 53 – 55: i.e. TECM key

(Transformed ECM key), as taught by Tsuria, which could be generated based

upon a combination of apparatus / device IRD and user-oriented smart card

information) and the En-Seung is relied upon providing an improved and more

efficient cryptographic process for the generation and use of encryption /

decryption keys in the transmission and replay of digital content; especially, in an

apparatus with terminal unit capable to directly descrambled the protected digital

content (without the need to transfer the received / encrypted digital content back

to the first device for decrypting) for replaying the digital information and thereby,

allows the clients to view the digital content at their convenience (En-Seung :

Column 2 Line 6 – 8, Column 1 Line 19 – 20 and Column 6 Line 8 – 13) and as

such the ordinary skill in the art can recognize the transfer of the decryption key

(i.e. a rebundled descrambling key, as taught by Tsuria) directly to the 2nd device

enables the terminal unit (2nd device) to <u>directly</u> descrambled the protected digital

content. Therefore, Examiner notes such a feature of "receiving, in said second

device, said scrambled data component and said rebundled descrambling key" is

lacking of the significance of patentability in view of En-Seung and Tsuria.

- As per new claim 23, the claim limitations are met as the same reasons as

that set forth in rejecting claim 3 – Examiner notes, first of all, the public / private

key pair should be used as a pair between the first device and the second device

– As far as which device (the 1st device or the 2nd device) uses the private key is

merely a obvious design choice in the art – for example, claim 3 and claim 23

recites using the public key and the private key at the first device (i.e. access

device) respectively (or <u>interchangeably</u>) and therefore Examiner notes this

claim feature holds no significance of the patentable feature.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1 – 5, 7, 8, 10, 14, 17 and 20 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Tsuria (U.S. Patent 6,178,242), in view of En-Seung et al.

(U.S. Patent 6,892,306).

        As per claim 1, Tsuria teaches a method for managing access, within a network

comprising a first device interconnected to a second device, the method comprising:

        (a) receiving said scrambled program in said first device, said scrambled

program comprising a scrambled data component and a descrambling key (Tsuria:

Column 3 Line 1 – 8 and Figure 1: the first device is interpreted as the IRD (Integrated

Receiver Decoder) on Figure 1 / Element 110 and the second device is interpreted as

the playback device (or VCR) on Figure 1 / Element 130 capable to record and present

data for display on the monitor);

        (b) rebundling, in said first device, said descrambling key using a unique key

associated with said first device (Tsuria: Column 3 Line 1 – 8 and Column 8 Line 53 –

55: i.e. TECM key (Transformed ECM key), as taught by Tsuria, which could be

generated based upon a combination of apparatus / device IRD and user-oriented smart

card information).

        Tsuria teaches receiving, in said second device, said scrambled data component

(Tsuria: Column 9 Line 30 – 36). However, Tsuria does not explicitly disclose receiving,

in said second device, said rebundled descrambling key.

        En-Seung teaches:

(c) receiving, in said second device, said scrambled data component and said

rebundled descrambling key (En-Seung: Column 2 Line 6 – 8, Column 4 Line 58 – 63,

Column 3 Line 9 – 13, Column 6 Line 37 – 40 / Line 8 –13, Column 1 Line 19 – 20 and

Abstract / Line 10 – 18: Examiner notes En-Seung provides an improved and more

efficient cryptographic process for the generation and use of encryption / decryption

keys in the transmission and replay of digital content; especially, in an apparatus with

terminal unit capable to <u>directly</u> descrambled the protected digital content (without the

need to transfer the received / encrypted digital content back to the first device for

decrypting) for replaying the digital information and thereby, allows the clients to view

the digital content at their convenience; where a "rebundled descrambling key" is

considered as an "encrypted content key" and the content key is considered as a

temporary validation key that encrypts the digital content. En-Seung teaches the first

device (i.e. the server) can also generate the key information related to the users in the

decryption process as well as in the encryption process (En-Seung: Column 4 Line 58 –

63). Besides, the user is the customer for both of the 1st device (e.g., IRD or Setup Box)

as well as the 2nd device (e.g., presentation device) and therefore the user (customer)

information or the user (customer) key is indeed associated with both of the 1st device

and the 2nd device in view of the TECM key (i.e. transformed ECM key or rebundled

descrambling key). Besides, En-Seung teaches the first device (i.e. the server or the

access device) can also generate the key information related to the users in the

decryption process as well as in the encryption process (En-Seung: Column 4 Line 58 –

63) in correspondence with the user's (i.e. customer's) identity characters for the

terminal unit (i.e. the 2nd device or the presentation device). Therefore, the TECM key

(i.e. a rebundled descrambling key) is not only associated with the 1st device but also

associated with the 2nd device as a whole to enable the encryption / decryption functions

work seamlessly – please refer to the section of Response to Argument).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of En-Seung within the system of Tsuria

because (a) Tsuria teaches protection mechanisms for producing, recording and

replaying scrambled digital data stream (Tsuria: Column 1 Line 60 – 63) and (b) En-

Seung teaches providing an improved and more efficient cryptographic process for the

generation and use of keys in the transmission and replay of digital content; especially,

in an apparatus with terminal unit capable to directly descrambled the protected digital

content, wherein the terminal unit is constructed with a personal computer PC equipped

with a peripheral accessory to the computer, such as compact disk drive or DVD for

replaying the digital information and thereby, allows the clients to view the digital

content at their convenience (En-Seung : Column 2 Line 6 – 8, Column 1 Line 19 – 20

and Column 6 Line 8 – 13).

(d) obtaining in said second device said descrambling key from said rebundled

descrambling key (En-Seung : Abstract / Line 10 – 14 and Column 8 Line 23 – 29 &

comment on (c)); and

(e) descrambling, in said second device, said scrambled data component using

said descrambling key (En-Seung : Abstract / Line 10 – 14 and Column 8 Line 23 – 29

& comment on (c)).

As per claim 2, Tsuria teaches (a) decrypting said encrypted descrambling key

using a key associated with said scrambled program; and (b) re-encrypting said

descrambling key using said unique key associated with said first device to produce

said rebundled descrambling key (Tsuria: Column 10 Line 36 – 40).

As per claim 3, Tsuria teaches said unique key associated with said first device is

a public key, said public key being located in said first device and a corresponding

private key being located in said second device (Tsuria: Column 3 Line 1 – 8, Column 8

Line 53 – 55 and Column 7 Line 5: See commonly assigned <both are from the same

assignee NDS Ltd. Inc.> and fully incorporated into Tsuria by reference the U.S. Patent

5,481,609, to Cohen et al., Column 1 Line 62 – 67).

As per claim 4, Tsuria teaches the step of rebundling is performed within a first

smart card coupled to said first device (Tsuria: Column 7 Line 1 – 9 and Column 6 Line

66 – Column 7 Line 1) and the steps of obtaining and descrambling are performed

within a second smart card coupled to said second device (Tsuria: Column 7 Line 5:

See commonly assigned <both are from the same assignee NDS Ltd. Inc.> and fully

incorporated into Tsuria by reference the U.S. Patent 5,481,609, to Cohen et al., Figure

3 Element 30 / 32 and Column 178 Line 21 – 23).

As per claim 5, Tsuria teaches initializing said first device within said network

(Tsuria: Column 8 Line 29 – 43 & Figure 1: the first device is IRD (Integrated Recording

Decoder) which directly interfaces with the SDDS broadcasting system to discourage

unauthorized duplication and subsequent play-back / recording).

As per claim 7, Tsuria as modified teaches a re-encryption key is pre-stored in a

smart card coupled to said first device or in said first device (Tsuria: Column 8 Line 30 –

31). Tsuria further teaches a re-encryption key is a public key (Tsuria: Column 3 Line 1

– 8, Column 8 Line 53 – 55 and Column 7 Line 5: See commonly assigned < both are

from the same assignee NDS Ltd. Inc.> and fully incorporated into Tsuria by reference the

U.S. Patent 5,481,609, to Cohen et al., Column 1 Line 62 – 67).

Accordingly, Tsuria as modified teaches:

a public key is pre-stored in a smart card coupled to said first device or in said

first device.

As per claim 8, Tsuria teaches said descrambling key is one of encrypted using a

private means if said scrambled program is received from prerecorded media or

protected by a private means if said scrambled program is received from a service

provider (Tsuria: Column 7 Line 50 – 57).

As per claim 10, Tsuria teaches a method for managing access to a scrambled

program received from a service provider within a network having an access device and

a presentation device, said method comprising:

(a) receiving said scrambled program in an access device, said scrambled

program comprising a scrambled data component and an encrypted descrambling key

(Tsuria: Column 3 Line 1 – 8 and Figure 1: the first device is interpreted as the IRD

(Integrated Receiver Decoder) on Figure 1 / Element 110 and the second device is

interpreted as the playback device (or VCR) on Figure 1 / Element 130 capable to

record and present data for display on the monitor);

(b) decrypting, in said access device, said encrypted descrambling key using a

key associated with said service provider (Tsuria: Column 3 Line 1 – 8 and Column 3

Line 11 – 16);

(c) re-encrypting said descrambling key, in said access device, using a public key

associated with said access device (Tsuria: Column 3 Line 1 – 8, Column 8 Line 53 –

55 and Column 7 Line 5: See commonly assigned < both are from the same assignee NDS Ltd.

Inc.> and fully incorporated into Tsuria by reference the U.S. Patent 5,481,609, to Cohen

et al., Column 1 Line 62 – 67).

Tsuria teaches receiving, in said presentation device, said scrambled

data-component (Tsuria: Column 9 Line 30 – 36 and Column 10 Line 21 – 40).

However, Tsuria does not explicitly disclose receiving, in said second device, said

rebundled descrambling key.

En-Seung teaches:

(d) receiving, in said presentation device, said scrambled data-component and

said re-encrypted descrambling key (En-Seung: Column 2 Line 6 – 8, Column 4 Line 58

– 63, Column 3 Line 9 – 13, Column 6 Line 37 – 40 / Line 8 –13, Column 1 Line 19 – 20

and Abstract / Line 10 – 18: Examiner notes En-Seung provides an improved and more

efficient cryptographic process for the generation and use of encryption / decryption

keys in the transmission and replay of digital content; especially, in an apparatus with terminal unit capable to <u>directly</u> descrambled the protected digital content (without the need to transfer the received / encrypted digital content back to the first device for decrypting) for replaying the digital information and thereby, allows the clients to view the digital content at their convenience; where a "rebundled descrambling key" is considered as an "encrypted content key" and the content key is considered as a temporary validation key that encrypts the digital content. En-Seung teaches the first device (i.e. the server) can also generate the key information related to the users in the decryption process as well as in the encryption process (En-Seung: Column 4 Line 58 – 63). Besides, the user is the customer for both of the 1st device (e.g., IRD or Setup Box) as well as the 2nd device (e.g., presentation device) and therefore the user (customer) information or the user (customer) key is indeed associated with both of the 1st device and the 2nd device in view of the TECM key (i.e. transformed ECM key or rebundled descrambling key). Besides, En-Seung teaches the first device (i.e. the server or the access device) can also generate the key information related to the users in the decryption process as well as in the encryption process (En-Seung: Column 4 Line 58 – 63) in correspondence with the user's (i.e. customer's) identity characters for the terminal unit (i.e. the 2nd device or the presentation device). Therefore, the TECM key (i.e. a rebundled descrambling key) is not only associated with the 1st device but also associated with the 2nd device as a whole to enable the encryption / decryption functions work seamlessly – please refer to the section of Response to Argument). See same rationale of combination applied herein as above in rejecting the claim 1.

(e) decrypting, in said presentation device, said re-encrypted descrambling key to

obtain said descrambling key (En-Seung : Abstract / Line 10 – 14 and Column 8 Line 23

– 29 & comment on (d)); and

(f) descrambling, in said presentation device, said scrambled data component

using said descrambling key (En-Seung : Abstract / Line 10 – 14 and Column 8 Line 23

– 29 & comment on (c));

As per claim 14, Tsuria as modified further teaches the first device is an access

device and wherein the second device is a presentation device (Tsuria: Figure 1,

Column 3 Line 1 – 8 and En-Seung: Column 3 Line 9 – 13, Column 6 Line 37 – 40 and

Abstract / Line 10 – 18).

As per claim 17, the claim limitation(s) encompasses the same scope as

described in claim 1 and claim 3 (Examiner notes the access device is considered as

the first device and the presentation device is considered as the second device). See

same rationale addressed above in rejecting claim 1 and claim 3.

As per claim 20, Tsuria as modified teaches the signal output transmits

identification data associated with the access device and copy control information along

with the re-encrypted descrambling key (Tsuria: Column 1 Line 60 – 67 and Column 2

Line 63 – Column 3 Line 5).

As per claim 21, Tsuria in view of En-Seung teaches the limitation that

encompasses the same scope at least as described in claim 1 – i.e., the claim 21

recites rebundling by the access device the descrambling information using key

information associated with the access device while the claim 1 recites rebundling, in

said first device, said descrambling key using a unique key associated with said first

device. Examiner notes in the encryption / decryption mechanism, the 1st device and

the 2nd device are functionally bundled together in order to encrypt / decrypt the digital

content – i.e. both of then can not be separated and functioned independently. Besides,

the user is the customer for both of the 1st device (e.g., IRD or Setup Box) as well as the

2nd device (e.g., presentation device) and therefore the user (customer) information or

the user (customer) key is indeed associated with both of the 1st device and the 2nd

device in view of the TECM key (i.e. transformed ECM key or rebundled descrambling

key). Besides, En-Seung teaches the first device (i.e. the server or the access device)

can also generate the key information related to the users in the decryption process as

well as in the encryption process (En-Seung: Column 4 Line 58 – 63) in correspondence

with the user's (i.e. customer's) identity characters for the terminal unit (i.e. the 2nd

device or the presentation device) and Tsuria teaches TECM key may be associated

with a combination of the IRD (i.e. the 1st device) as well as a smart card and the TECM

key may be personal to a particular user (customer) of the apparatus (i.e. the 1st device

(or access device) and the 2nd device (i.e. the presentation device) (Tsuria: Column 8

Line 53 – 62) and as such Tsuria in view of En-Seung does teach "rebundling by the

access device the descrambling information using key information associated with the

access device".

As per claim 22, Tsuria as modified teaches the key information corresponding to

entitlement control messages, and further comprises the key information corresponds to

entitlement control messages, and further comprising the step of obtaining a

descrambling key from the entitlement control messages, and the descrambling step

comprises descrambling the program signal using the descrambling key (Tsuria:

Column 7 Line 48 – 57).

As per claim 23, the claim limitations are met as the same reasons as that set

forth above in rejecting claim 3 – Examiner notes, first of all, the public / private key pair

should be used as a pair between the first device and the second device; as far as

which device (the 1st device or the 2nd device) uses the private key is merely a obvious

design choice – for example, claim 3 and claim 23 recites using the public key and the

private key at the first device (i.e. access device) respectively (or interchangeably) and

therefore Examiner notes this claim feature holds no significance of the patentable

feature).

As per claim 24, the claim limitations are met as the same reasons as that set

forth above in rejecting claim 19.

4.   Claims 6 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Tsuria (U.S. Patent 6,178,242), in view of En-Seung et al. (U.S. Patent 6,892,306), and

in view of Wasilewski et al. (U.S. Patent 5,870,474).

        As per claim 6, Tsuria as modified does not disclose expressly initializing

comprises the step of receiving a public key from a conditional access provider.

        Wasilewski teaches initializing comprises the step of receiving a public key from

a conditional access provider (Wasilewski: Column 3 Line 53 – 67 and Column 7 Line

38 – 43).

        It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Wasilewski within the system of Tsuria

as modified because (a) Tsuria teaches protection mechanisms for producing, recording

and replaying scrambled digital data stream (Tsuria: Column 1 Line 60 – 63) and (b)

Wasilewski teaches a control system for providing secure transmission of recording

digital data stream (such as "movie on demand") between a service provider and a

customer's set top box over a digital network (Wasilewski: Column 1 Line 15 – 25).

        Accordingly, Tsuria as modified teaches:

        the step of initializing comprises the step of receiving said public key from a

conditional access provider (Wasilewski: Column 3 Line 53 – 67 and Column 7 Line 38

– 43), said step of receiving comprising authentication of said conditional access

provider (Wasilewski: Column 11 Line 4 – 5; Tsuria: Column 8 Line 30 – 31).

As per claim 18, Tsuria as modified does not teach the public key is periodically

received from a conditional access provider.

Wasilewski teaches the public key is periodically received from a conditional

access provider (Wasilewski: Column 7 Line 38 – 40 and Column 10 Line 4 – 12). See

same rationale of combination applied herein as above in rejecting the claim 6.

5.   Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria

(U.S. Patent 6,178,242), in view of En-Seung et al. (U.S. Patent 6,892,306), and in view

of Smyers et al. (U.S. Patent 5,948,136).

As per claim 19, Tsuria as modified does not teach the signal output

authenticates the presentation device before transmitting the scrambled data

component and the re-encrypted descrambling key to the presentation device.

Smyers the signal output authenticates the presentation device before

transmitting the scrambled data component and the re-encrypted descrambling key to

the presentation device (Smyers: Column 4 Line 38 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Smyers within the system of Tsuria as

modified because (a) Tsuria teaches protection mechanisms for producing, recording

and replaying scrambled digital data stream (Tsuria: Column 1 Line 60 – 63) and (b)

Smyers teaches providing hardware authentication mechanism to enhance

communication securities between two devices.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.
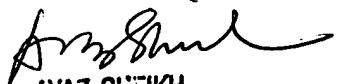
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100